MODELING AND ANALYSIS OF INFORMATION SYSTEMS, VOL. 28, NO. 2, 2021
journal homepage: www.mais-journal.ru

ALGORITHMS

Computational Analysis of Quantitative Characteristics of some Residual Properties of Solvable Baumslag–Solitar Groups

E. A. Tumanova[1]

DOI: 10.18255/1818-1015-2021-2-136-145

[1]Ivanovo State University, 39 Ermak str., Ivanovo 153025, Russia.

MSC2020: Primary 68R05, 20E26, 62-07. Secondary 68Q25, 20F05, 62-04
Research article
Full text in Russian

Received April 26, 2021
After revision May 28, 2021
Accepted June 2, 2021

Let G_k be defined as $G_k = \langle a, b;\ a^{-1}ba = b^k \rangle$, where $k \neq 0$. It is known that, if p is some prime number, then G_k is residually a finite p-group if and only if $p \mid k-1$. It is also known that, if p and q are primes not dividing $k-1$, $p < q$, and $\pi = \{p, q\}$, then G_k is residually a finite π-group if and only if $(k, q) = 1$, $p \mid q-1$, and the order of k in the multiplicative group of the field $\mathbb{Z}_q$ is a p-number. This paper examines the question of the number of two-element sets of prime numbers that satisfy the conditions of the last criterion. More precisely, let $f_k(x)$ be the number of sets $\{p, q\}$ such that $p < q$, $p \nmid k-1$, $q \nmid k-1$, $(k, q) = 1$, $p \mid q-1$, the order of k modulo q is a p-number, and p, q are chosen among the first x primes. We state that, if $2 \leq |k| \leq 10000$ and $1 \leq x \leq 50000$, then, for almost all considered k, the function $f_k(x)$ can be approximated quite accurately by the function $\alpha_k x^{0.85}$, where the coefficient α_k is different for each k and $\{\alpha_k \mid 2 \leq |k| \leq 10000\} \subseteq (0.28;\ 0.31]$. We also investigate the dependence of the value $f_k(50000)$ on k and propose an effective algorithm for checking a two-element set of prime numbers for compliance with the conditions of the last criterion. The results obtained may have applications in the theory of computational complexity and algebraic cryptography.

Keywords: Baumslag–Solitar groups; residual π-finiteness; function approximation; analysis of algorithms

INFORMATION ABOUT THE AUTHORS

Elena Alexandrovna Tumanova
correspondence author

orcid.org/0000-0002-6193-9834. E-mail: helenfog@bk.ru
Associate Professor, Ph. D. in Mathematics.

For citation: E. A. Tumanova, "Computational Analysis of Quantitative Characteristics of some Residual Properties of Solvable Baumslag–Solitar Groups", *Modeling and analysis of information systems*, vol. 28, no. 2, pp. 136-145, 2021.

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ, ТОМ 28, № 2, 2021
сайт журнала: www.mais-journal.ru

Вычислительный анализ количественных характеристик некоторых аппроксимационных свойств разрешимых групп Баумслага–Солитэра

Е. А. Туманова[1]

DOI: 10.18255/1818-1015-2021-2-136-145

[1]Ивановский государственный университет, ул. Ермака, д. 39, г. Иваново, 153025 Россия.

УДК 004.421, 512.54, 519.25, 519.65
Научная статья
Полный текст на русском языке

Получена 26 апреля 2021 г.
После доработки 28 мая 2021 г.
Принята к публикации 2 июня 2021 г.

Пусть $G_k = \langle a, b;\ a^{-1}ba = b^k \rangle$, где $k \neq 0$. Известно, что если p — некоторое простое число, то группа G_k аппроксимируется конечными p-группами тогда и только тогда, когда $p \mid k - 1$. Известно также, что если p и q — простые числа, не делящие $k - 1$, $p < q$ и $\pi = \{p,\ q\}$, то группа G_k аппроксимируется конечными π-группами тогда и только тогда, когда $(k, q) = 1$, $p \mid q - 1$ и порядок числа k в мультипликативной группе поля $\mathbb{Z}_q$ является p-числом. В настоящей статье исследуется вопрос о количестве двухэлементных множеств простых чисел, удовлетворяющих условиям последнего критерия. Более точно, пусть $f_k(x)$ — количество множеств $\{p,\ q\}$ таких, что $p < q$, $p \nmid k - 1$, $q \nmid k - 1$, $(k, q) = 1$, $p \mid q - 1$, порядок k по модулю q является p-числом и p, q выбираются среди первых x простых чисел. Установлено, что если $2 \leq |k| \leq 10000$ и $1 \leq x \leq 50000$, то почти для всех рассматриваемых k функция $f_k(x)$ может быть достаточно точно приближена функцией $\alpha_k x^{0,85}$, где коэффициент α_k — свой для каждого k и $\{\alpha_k \mid 2 \leq |k| \leq 10000\} \subseteq (0,28;\ 0,31]$. Также исследована зависимость величины $f_k(50000)$ от k и предложен эффективный алгоритм проверки двухэлементного множества простых чисел на соответствие условиям последнего критерия. Полученные результаты могут иметь приложения в теории сложности вычислений и алгебраической криптографии.

Ключевые слова: группы Баумслага–Солитэра; аппроксимируемость конечными π-группами; аппроксимация функций; анализ алгоритмов

ИНФОРМАЦИЯ ОБ АВТОРАХ

Елена Александровна Туманова
автор для корреспонденции
orcid.org/0000-0002-6193-9834. E-mail: helenfog@bk.ru
доцент, канд. физ.-мат. наук.

Для цитирования: E. A. Tumanova, “Computational Analysis of Quantitative Characteristics of some Residual Properties of Solvable Baumslag–Solitar Groups”, *Modeling and analysis of information systems*, vol. 28, no. 2, pp. 136-145, 2021.

1. Некоторые аппроксимационные свойства рассматриваемых групп

Следуя [1], для каждого ненулевого целого числа k обозначим через G_k группу, которая задается представлением $G_k = \langle a, b;\ a^{-1}ba = b^k \rangle$. Она входит в хорошо известное семейство групп Баумслага–Солитэра $\mathrm{BS}(m, n) = \langle a, b;\ a^{-1}b^m a = b^n \rangle$, где m и n — ненулевые целые числа.

Изучение аппроксимационных свойств группы G_k было начато Г. Баумслагом и Д. Солитэром в [2]. Напомним, что группа G называется *аппроксимируемой классом групп* $\mathcal{C}$ (*$\mathcal{C}$-аппроксимируемой*), если для любого неединичного элемента $g \in G$ существует гомоморфизм φ группы G на группу из класса $\mathcal{C}$ такой, что $g\varphi \neq 1$. В [2, 3] установлено, что группа G_k финитно аппроксимируема, то есть аппроксимируема классом всех конечных групп. Исследование аппроксимируемости этой группы конечными группами было продолжено Д. И. Молдаванским. В [4] он доказал следующий критерий аппроксимируемости группы G_k классом $\mathcal{F}_p$ всех конечных p-групп, где p — некоторое простое число.

Теорема 1. [4, теорема 3] *Пусть p — простое число. Группа G_k $\mathcal{F}_p$-аппроксимируема тогда и только тогда, когда p делит $k - 1$.*

В [5] была рассмотрена аппроксимируемость группы G_k классом $\mathcal{F}_\pi$ всех конечных π-групп, где π — некоторое множество простых чисел. Напомним, что целое число называется *π-числом*, если все его простые делители принадлежат множеству π, периодическая группа называется *π-группой*, если порядки всех ее элементов являются π-числами. Приводимая далее теорема 2 дает критерий аппроксимируемости группы G_k конечными π-группами для произвольного множества π простых чисел. Поясним, что в ее формулировке и всюду далее под порядком целого числа x по модулю целого числа y понимается порядок числа x в мультипликативной группе кольца $\mathbb{Z}_y$.

Теорема 2. [5, теорема 1] *Пусть π — произвольное множество простых чисел. Группа G_k $\mathcal{F}_\pi$-аппроксимируема тогда и только тогда, когда существует π-число $s > 1$, взаимно простое с k, порядок по модулю которого числа k также является π-числом.*

Критерий, содержащийся в теореме 2, не является конструктивным, т. е. не дает алгоритма, позволяющего для заданных числа k и множества π проверить, аппроксимируется ли группа G_k классом $\mathcal{F}_\pi$. Такой алгоритм существует для двухэлементного множества простых чисел и предоставляется приводимой далее теоремой 3. Отметим, что в этой теореме рассматриваются только пары простых чисел p и q, каждое из которых не делит $k - 1$, поскольку в противном случае группа G_k аппроксимируется классом $\mathcal{F}_p$ или $\mathcal{F}_q$ согласно теореме 1.

Теорема 3. [5, теорема 2] *Пусть p и q — простые числа, удовлетворяющие условиям*

a) $p < q$;

b) $p \nmid k - 1$;

c) $q \nmid k - 1$.

Пусть также $\pi = \{p, q\}$. Группа G_k $\mathcal{F}_\pi$-аппроксимируема тогда и только тогда, когда

1) $(k, q) = 1$;

2) $p \mid q - 1$;

3) *порядок k по модулю q является p-числом.*

Хотя теорема 3 имеет эффективно проверяемое условие, она не дает ответа на вопрос, для всех ли значений k существует пара простых чисел (p, q), удовлетворяющая ее условию. Нетрудно проверить, что при $k = \pm 1$ такой пары нет. При $|k| > 1$ наличие пары простых чисел с требуемыми свойствами устанавливает

Теорема 4. [5, теорема 3] *Если $|k| > 1$, то для любого простого числа p, не делящего $k - 1$, найдется простое число q, не делящее $k - 1$ и такое, что группа G_k $\mathcal{F}_\pi$-аппроксимируема, где $\pi = \{p, q\}$.*

Теорема 4 оставляет открытым вопрос о количестве двухэлементных множеств простых чисел, удовлетворяющих условиям теоремы 3. В данной работе этот вопрос исследуется при условии, что $2 \le |k| \le 10000$ и элементы множества выбираются из первых 50000 простых чисел. Указанные ограничения обусловлены временем работы программы, перечисляющей двухэлементные множества простых чисел и выбирающей из них те, для которых справедливы условия теоремы 3. Попытка дальнейшего увеличения диапазона рассматриваемых простых чисел приводит к несоразмерному росту времени выполнения расчетов исходных данных для проведения исследования; подробнее об этом см. в разделе 4.

2. Зависимость от k числа двухэлементных множеств, удовлетворяющих условиям теоремы 3

Пусть $|k| > 1$ и $n \ge 1$. Будем использовать следующие обозначения:

$\mathcal{P}(n)$ — множество, составленное из первых n простых чисел;

$S_k(n)$ — множество пар простых чисел (p, q), удовлетворяющих условиям a–c, 1–3 теоремы 3 и таких, что $p, q \in \mathcal{P}(n)$;

$f_k(n)$ — мощность множества $S_k(n)$.

Положим также

$$\mathcal{K} = \{-10000; -2\} \cup \{2; 10000\}, \quad \mathfrak{C}(k) = f_k(50000), \quad \mathfrak{c}(k) = f_k(4).$$

Посредством явного вычисления элементов множеств $S_k(50000)$ при $2 \le |k| \le 10000$ было установлено, что значения $\mathfrak{C}(k)$ меняются в достаточно широких пределах. Если рассматривать функцию $\mathfrak{C} : \mathcal{K} \longrightarrow \mathbb{Z}$ как случайную величину, то в предположении равновероятности всех элементарных событий имеем

$$M(\mathfrak{C}) \approx 2940,57; \quad \sigma(\mathfrak{C}) \approx 280,02.$$

Можно выделить некоторые значения k, для которых величина $\mathfrak{C}(k)$ существенно отличается от $M(\mathfrak{C})$. Неравенство $\mathfrak{C}(k) < \frac{1}{2}M(\mathfrak{C})$ выполняется для 76 элементов множества $\mathcal{K}$, причем все эти числа отрицательны. Среди них следует особо отметить те значения k, для которых $\mathfrak{C}(k) < \frac{1}{4}M(\mathfrak{C})$: -256; -16; -6561; -4096; -576; -9216; -2916. Все положительные значения $k \in \mathcal{K}$ удовлетворяют соотношению $\mathfrak{C}(k) > 0,73M(\mathfrak{C})$.

В случае с превышением величиной $\mathfrak{C}(k)$ среднего значения $M(\mathfrak{C})$ картина складывается прямо противоположная. Неравенство $\mathfrak{C}(k) > 2M(\mathfrak{C})$ выполняется для 37 значений k, и все они положительны. Нельзя не обратить внимание на $k = 4096$, так как $\mathfrak{C}(4096) = 11878 > 4M(\mathfrak{C})$ и $\mathfrak{C}(k) < 3M(\mathfrak{C})$ для всех остальных $k \in \mathcal{K}$. Все отрицательные значения $k \in \mathcal{K}$ удовлетворяют соотношению $\mathfrak{C}(k) < 1,62M(\mathfrak{C})$.

Точки, в которых функция $\mathfrak{C}(k)$ принимает 20 самых больших и 20 самых маленьких значений, приводятся в табл. 1. Анализируя ее содержимое, логично предположить, что значение функции $\mathfrak{C}(k)$ существенным образом связано с разложением числа k на простые множители. Изучение такой зависимости может стать предметом дальнейших исследований.

Еще один естественным образом возникающий вопрос — можно ли довольно быстро вручную найти пару простых чисел, удовлетворяющих условиям теоремы 3. Для ответа на него была исследована функция $\mathfrak{c}(k)$, соответствующая случаю, когда простые числа выбираются из множества $\mathcal{P}(4) = \{2, 3, 5, 7\}$.

Установлено, что для 10000 из 19998 рассмотренных значений k справедливо неравенство $\mathfrak{c}(k) > 0$, причем среди этих 10000 значений k положительных и отрицательных практически поровну: 4998 положительных и 5002 отрицательных. Таким образом, примерно для половины элементов множества $\mathcal{K}$ искомую пару простых чисел можно быстро найти подбором. Кроме этого, установлено, что $\mathfrak{c}(k) \le 3$ для любого $k \in \mathcal{K}$. Количества элементов множества $\mathcal{K}$, для которых функция $\mathfrak{c}(k)$ принимает значения 0, 1, 2, 3, приведены в табл. 2.

Table 1. The largest and smallest values of the function $\mathfrak{C}(k)$

Таблица 1. Наибольшие и наименьшие значения функции $\mathfrak{C}(k)$

k	$\mathfrak{C}(k)$	$\mathfrak{C}(k)/M(\mathfrak{C})$	k	$\mathfrak{C}(k)$	$\mathfrak{C}(k)/M(\mathfrak{C})$
−256	267	$\approx 0,091$	225	6038	$\approx 2,053$
−16	481	$\approx 0,164$	441	6049	$\approx 2,057$
−6561	570	$\approx 0,194$	100	6050	$\approx 2,057$
−4096	693	$\approx 0,236$	3600	6067	$\approx 2,063$
−576	727	$\approx 0,247$	9216	6243	$\approx 2,123$
−9216	732	$\approx 0,249$	576	6254	$\approx 2,127$
−2916	733	$\approx 0,249$	36	6277	$\approx 2,135$
−36	739	$\approx 0,251$	2916	6296	$\approx 2,141$
−2401	919	$\approx 0,313$	1024	6408	$\approx 2,179$
−625	935	$\approx 0,318$	81	6918	$\approx 2,353$
−10000	959	$\approx 0,326$	1296	6990	$\approx 2,377$
−81	1035	$\approx 0,352$	625	7175	$\approx 2,440$
−1296	1052	$\approx 0,358$	10000	7190	$\approx 2,445$
−100	1169	$\approx 0,398$	2401	7271	$\approx 2,473$
−1600	1187	$\approx 0,404$	64	7429	$\approx 2,526$
−8100	1194	$\approx 0,406$	6561	7947	$\approx 2,703$
−8427	1228	$\approx 0,418$	16	8206	$\approx 2,791$
−1587	1249	$\approx 0,425$	729	8306	$\approx 2,825$
−9075	1268	$\approx 0,431$	256	8660	$\approx 2,945$
−4107	1269	$\approx 0,432$	4096	11878	$\approx 4,039$

Table 2. Frequencies of the values of the function $\mathfrak{c}(k)$

Таблица 2. Частоты встречаемости значений функции $\mathfrak{c}(k)$

x	0	1	2	3
$\operatorname{card}\{k \in \mathcal{K} \mid \mathfrak{c}(k) = x\}$	9998	6285	2858	857

3. Зависимость числа двухэлементных множеств, удовлетворяющих условиям теоремы 3, от количества рассматриваемых простых чисел

В данном разделе исследуется вопрос о том, как меняется количество пар простых чисел, удовлетворяющих условию теоремы 3, т. е. величина $f_k(n)$, в зависимости от количества n рассматриваемых простых чисел при фиксированном k. Можно ли одной из элементарных функций довольно хорошо приблизить такую зависимость? Из результатов предыдущего параграфа ясно, что при различных k функции $f_k(x)$ имеют существенно различающиеся значения. Но влияет ли k на характер зависимости или функции $f_k(x)$ отличаются друг от друга лишь некоторым множителем?

Чтобы ответить на эти вопросы, вычисленные значения функций $f_k(x)$ были визуализированы для некоторых k (см. рис. 1). В результате возникло предположение о том, что при различных k функции $f_k(x)$ имеют один и тот же характер зависимости, похожий на логарифмический или степенной (с показателем степени, меньшим 1). Первые же попытки аппроксимации показали, что логарифмическая функция не подходит. Поэтому далее было решено искать приближенную функцию в виде $g_k(x) = \alpha x^\beta$, где коэффициенты α и β, вообще говоря, зависят от k.

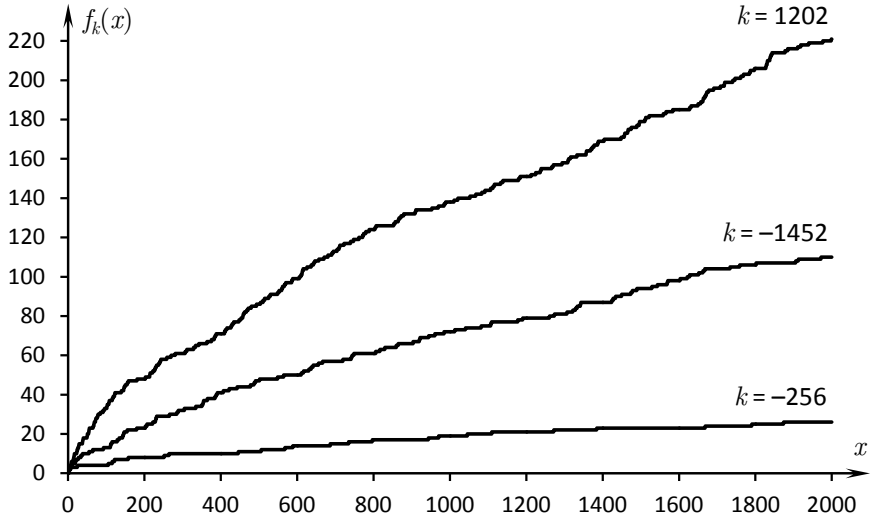

Fig. 1. The graph of the function $f_k(x)$ on the set $\{1, 2, \ldots, 2000\}$ for different k

Рис. 1. График функции $f_k(x)$ на множестве $\{1, 2, \ldots, 2000\}$ при различных k

При заданных k и β поиск множителя α выполнялся, исходя из условия

$$\sum_{x=1}^{50000} \left(1 - \frac{\alpha x^{\beta}}{\tilde{f}_k(x)}\right)^2 \to \min,$$

где

$$\tilde{f}_k(x) = \begin{cases} f_k(x), & \text{если } f_k(x) \neq 0, \\ 1, & \text{если } f_k(x) = 0, \end{cases}$$

откуда

$$\alpha = \left(\sum_{x=1}^{50000} x^{\beta}\right) \Bigg/ \left(\sum_{x=1}^{50000} \frac{x^{2\beta}}{\tilde{f}_k(x)}\right).$$

Определение β осуществлялось двумя способами.

Способ 1. Перебор для каждого $k \in \mathcal{K}$ всех значений из множества $\mathcal{B}$, содержащего числа от $0,7$ до $0,99$ с шагом $0,01$. Минимальный элемент множества $\mathcal{B}$ был найден в ходе предварительных расчетов с меньшим количеством точек, в которых вычислялись функции $f_k(x)$.

При фиксированном $k \in \mathcal{K}$ для каждого $b \in \mathcal{B}$ определялись соответствующие ему значения

$$\alpha(b) = \left(\sum_{x=1}^{50000} x^{b}\right) \Bigg/ \left(\sum_{x=1}^{50000} \frac{x^{2b}}{\tilde{f}_k(x)}\right), \qquad \delta(b) = \sum_{x=1}^{50000} \left(1 - \frac{\alpha(b) x^{b}}{\tilde{f}_k(x)}\right)^2,$$

после чего выбирался тот элемент $b \in \mathcal{B}$, для которого значение $\delta(b)$ оказалось минимальным. Этот элемент далее обозначается через β_k.

Способ 2. Использование для всех $k \in \mathcal{K}$ одного и того же элемента $b \in \mathcal{B}$.

Выбирался элемент $b \in \mathcal{B}$, наиболее близкий к среднему значению чисел β_k ($k \in \mathcal{K}$), полученных первым способом. Этот элемент далее обозначается через β_{avg}.

Отметим, что определение β с большей точностью не производилось, поскольку исходная задача состояла лишь в описании общего вида функций $f_k(x)$, а не в получении возможности отыскания

их значений с помощью аппроксимирующей функции $g_k(x)$. При этом найденное таким путем приближение оказалось вполне удовлетворительным (см. ниже).

Возможность выбора коэффициента β вторым способом обеспечивается особенностью распределения чисел β_k ($k \in \mathcal{K}$). Пусть функции $\beta : \mathcal{K} \to \mathcal{B}$ и $\eta : \mathcal{B} \to \mathbb{Z}$ определены следующим образом: $\beta(k) = \beta_k$, $\eta(b) = \operatorname{card}\{k \in \mathcal{K} \mid \beta(k) = b\}$. Значения функции η, представленные в табл. 3, позволяют сделать предположение о том, что функция β, рассматриваемая как дискретная случайная величина, имеет нормальное распределение. Проверим для нее выполнение правила «трех сигм».

Имеем $M(\beta) \approx 0,8531$ и $\sigma(\beta) \approx 0,0206$. Случайная величина $\beta(k)$ содержится в интервале $\big(M(\beta) - 3\sigma(\beta);\ M(\beta) + 3\sigma(\beta)\big)$ с вероятностью $\approx 0,9954$, в интервале $\big(M(\beta) - 2\sigma(\beta);\ M(\beta) + 2\sigma(\beta)\big)$ — с вероятностью $\approx 0,9531$, в интервале $\big(M(\beta) - \sigma(\beta);\ M(\beta) + \sigma(\beta)\big)$ — с вероятностью $\approx 0,6688$. Правило «трех сигм» не выполнено, но полученные вероятности лишь немного отличаются от необходимых значений, поэтому можно считать, что распределение случайной величины $\beta(k)$ близко к нормальному.

Table 3. Nonzero values of the function η **Таблица 3.** Ненулевые значения функции η

b	0,71	0,75	0,76	0,77	0,78	0,79	0,80	0,81	0,82	0,83	0,84
$\eta(b)$	1	1	2	4	14	16	71	337	1030	2297	3426
b		0,85	0,86	0,87	0,88	0,89	0,90	0,91	0,92	0,93	0,94
$\eta(b)$		3886	3457	2605	1566	793	323	115	37	11	6

Отметим, что два самых маленьких значения функции β соответствуют элементам множества $\mathcal{K}$ из табл. 1. Так, $\beta(k) = 0,71$ при $k = -256$ и $\beta(k) = 0,75$ при $k = -2916$. Что касается максимума функции $\beta(k) = 0,94$, то здесь ситуация обратная — в пяти точках из шести, где он достигается, случайная величина $\mathfrak{C}$ принимает значение, близкое к $M(\mathfrak{C})$. Исключение составляет $k = -1849$, для которого $\mathfrak{C}(k) = 1630$. Таким образом, явной взаимосвязи между точками, в которых функции $\mathfrak{C}$ и β принимают значения, близкие к предельным, не наблюдается.

При использовании способов 1 и 2 для каждого $k \in \mathcal{K}$ были найдены два значения коэффициента α; обозначим их через $\alpha_k^{(1)}$ и $\alpha_k^{(2)}$ соответственно и отметим, что

$$\big\{\alpha_k^{(1)} \bigm| k \in \mathcal{K}\big\} \subseteq \big[0,064;\ 0,775\big], \quad \big\{\alpha_k^{(2)} \bigm| k \in \mathcal{K}\big\} \subseteq \big[0,028;\ 1,186\big].$$

Чтобы описать распределение значений $\alpha_k^{(1)}$ и $\alpha_k^{(2)}$ более точно, введем функции

$$\mathfrak{A}^{(i)} : \mathcal{A} \to \mathbb{Z}, \quad \mathfrak{A}^{(i)}(a) = \operatorname{card}\big\{k \in \mathcal{K} \bigm| a - 0,01 < \alpha_k^{(i)} \le a\big\},$$

где $i \in \{1;\ 2\}$, $\mathcal{A} = \{0,01;\ 0,02;\ \ldots;\ 0,99;\ 1\}$. Графики этих функций в логарифмическом масштабе на множестве $\mathcal{A}' = \{0,1;\ 0,11;\ \ldots;\ 0,59;\ 0,6\}$ представлены на рис. 2. Отметим, что $\mathfrak{A}^{(1)}(a) \le 3$ и $\mathfrak{A}^{(2)}(a) \le 7$ при $a \notin \mathcal{A}'$.

Анализируя значения функций $\mathfrak{A}^{(1)}$ и $\mathfrak{A}^{(2)}$, можно сделать следующие выводы.

1. Подавляющее большинство (18997 из 19998) коэффициентов $\alpha_k^{(2)}$ принадлежит промежутку $(0,28;\ 0,31]$, при этом 12336 из них содержится в промежутке $(0,29;\ 0,30]$. Как следствие, при аппроксимации всех функций $f_k(x)$ можно попытаться использовать один и тот же коэффициент α, близкий к среднему значению чисел $\alpha_k^{(2)}$ ($k \in \mathcal{K}$).

2. Функция $\mathfrak{A}^{(1)}$ имеет несколько локальных максимумов, близких по величине и не превосходящих 2535. Поэтому в данном случае выбрать какое-то одно значение коэффициента α не представляется возможным.

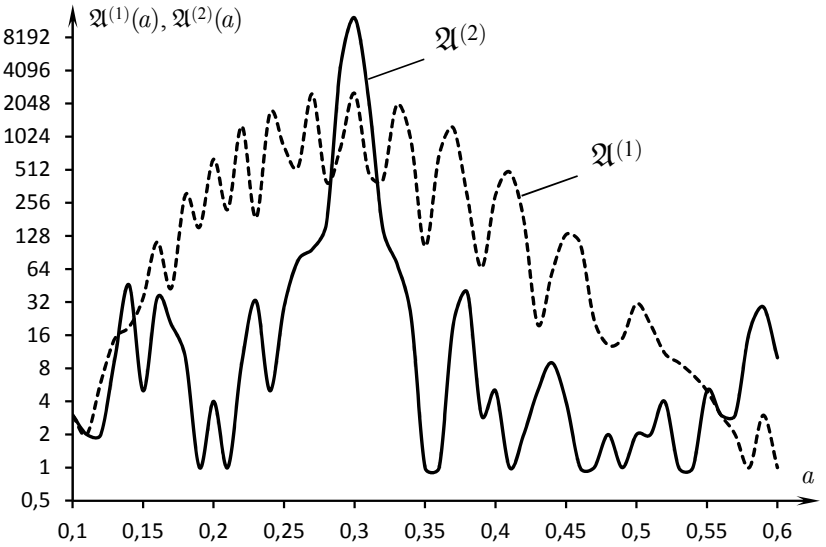

Fig. 2. The graphs of the functions $\mathfrak{A}^{(1)}(a)$ and $\mathfrak{A}^{(2)}(a)$

Рис. 2. Графики функций $\mathfrak{A}^{(1)}(a)$ и $\mathfrak{A}^{(2)}(a)$

Для каждого $k \in \mathcal{K}$ оценка качества аппроксимации функции $f_k(x)$ осуществлялась путем определения числа, ограничивающего сверху величины

$$\left|1 - g_k(x) \big/ \tilde{f}_k(x)\right| \quad \big(x \in \mathcal{P}(50000)\big)$$

по меньшей мере для 95% элементов множества $\mathcal{P}(50000)$. Будем говорить, что число $k \in \mathcal{K}$ обладает свойством $\mathfrak{P}(r)$, где $r \in (0;1)$, если

$$P\left\{\left|1 - g_k(x) \big/ \tilde{f}_k(x)\right| \le r\right\} \ge 0,95$$

или, что то же самое,

$$\operatorname{card}\left\{x \in \mathcal{P}(50000) \;\middle|\; \left|1 - g_k(x) \big/ \tilde{f}_k(x)\right| \le r\right\} \ge 47500.$$

В табл. 4 представлены сведения о количествах элементов множества $\mathcal{K}$, *не* обладающих свойством $\mathfrak{P}(r)$, в зависимости от способа вычисления коэффициента β. Как и следовало ожидать, применение первого способа дает лучшее приближение. Однако и при использовании второго способа большинство чисел из множества $\mathcal{K}$ обладает свойством $\mathfrak{P}(0,15)$, что также можно считать вполне удовлетворительным результатом.

Естественно предположить, что если для некоторого $k \in \mathcal{K}$ величина β_k существенно отличается от β_{avg}, то функция $g_k(x) = \alpha_k^{(2)} x^{\beta_{avg}}$ не очень хорошо приближает функцию $f_k(x)$ и потому свойство $\mathfrak{P}(r)$ выполняется для числа k лишь при достаточно большом r. Тем не менее, соответствия между величиной $|\beta_k - \beta_{avg}|$ и минимальным $r \in (0;1)$, для которого k обладает свойством $\mathfrak{P}(r)$, выявлено не было.

Table 4. The numbers of elements of $\mathcal{K}$ that do not have the property $\mathfrak{P}(r)$

Таблица 4. Количества элементов $\mathcal{K}$, не обладающих свойством $\mathfrak{P}(r)$

r	0, 08	0, 09	0, 10	0, 11	0, 12	0, 13	0, 14	0, 15	0, 16	0, 17	0, 18	0, 19	0, 20
Способ 1	226	100	52	26	17	8	5	3	2	1	1	0	0
Способ 2	1860	1091	670	383	233	133	79	55	35	24	14	5	4

Итак, проведенный анализ позволяет сделать следующий

Вывод. *Почти для всех* $k \in \mathcal{K}$ *функция* $f_k(x)$ *на множестве* $\{1, 2, \ldots, 50000\}$ *может быть с достаточной точностью приближена функцией* $g_k(x) = \alpha_k x^{\beta}$, *где* $\beta = \beta_{avg} = 0,85$ *и* $0,28 < \alpha_k \leq 0,31$.

4. О вычислительной сложности проверки условий теоремы 3

Все описанные выше результаты получены с помощью программ, реализованных автором на языке C++ (GCC) с использованием C RTL и C++ STL. Из произведенных расчетов наибольшую вычислительную сложность имело отыскание элементов множества $S_k(n)$. Для выполнения этой операции требуется проверить на соответствие условиям теоремы 3 $\frac{n(n-1)}{2}$ пар (p, q), где $p < q$. В ходе каждой такой проверки необходимо убедиться в том, что

1) p не делит $k - 1$;
2) q не делит $k - 1$;
3) $(k, q) = 1$ (что ввиду простоты числа q равносильно условию $q \nmid k$);
4) p делит $q - 1$;
5) порядок k по модулю q является p-числом.

Очевидно, что первые четыре операции могут быть выполнены процессором за время $O(1)$. Если следовать математической формулировке последней операции, то необходимо

а) вычислить порядок числа k по модулю q;
б) проверить, является ли он степенью числа p.

Напомним, что порядок k по модулю q — это наименьшее число x из множества $\{0, 1, \ldots, q-1\}$, удовлетворяющее соотношению $k^x \equiv 1 \pmod{q}$. Таким образом, отыскание порядка числа k — это не что иное, как вычисление дискретного логарифма в мультипликативной группе поля $\mathbb{Z}_q$. Как известно, данная задача является достаточно трудоемкой: распространенные алгоритмы ее решения имеют сложность порядка $O(\sqrt{q})$.

Чтобы сделать алгоритм более эффективным, заметим, что в действительности нам не нужно вычислять порядок s числа k, а достаточно лишь проверить, является ли он p-числом. Пусть m — максимальное целое число, удовлетворяющее соотношению $p^m \mid q - 1$. Так как рассматриваемая группа имеет порядок $q - 1$, то $s \mid q - 1$ и, значит, порядок s является p-числом тогда и только тогда, когда он совпадает с одним из чисел $1, p, p^2, \ldots, p^m$. При этом $s \neq 1$, поскольку q не делит $k - 1$.

Таким образом, для выполнения последней, пятой, операции необходимо $m \leq \log_p(q-1)$ проб. Каждая из них требует возвести в степень p либо число k (для первой пробы), либо число, рассмотренное при предыдущей пробе. При использовании бинарного алгоритма возведения в степень (см., например, [6, § 1.2]) для этого требуется порядка $O(\ell)$ умножений, где $\ell = \lfloor \log_2 p \rfloor + 1$ — длина битового представления числа p. В итоге, предложенный алгоритм проверки пары (p, q) на соответствие условиям теоремы 3 имеет сложность

$$O(\log_2 p \cdot \log_p q) = O(\log_2 q),$$

меньшую, чем при вычислении дискретного логарифма.

References

[1] D. I. Moldavanski and N. Y. Sibyakova, “On the finite images of some one-relator groups”, *Proc. Amer. Math. Soc.*, vol. 123, 2017–2020, 1995.

[2] G. Baumslag and D. Solitar, “Some two-generator one-relator non-Hopfian groups”, *Bull. Amer. Math. Soc.*, vol. 68, 199–201, 1962.

[3] S. Meskin, “Nonresidually finite one-relator groups”, *Trans. Amer. Math. Soc.*, vol. 164, 105–114, 1972.

[4] D. I. Moldavanskii, "The residual p-finiteness of HNN-extensions", *Bull. Ivanovo State Univ.*, no. 3, 129–140, 2000.

[5] O. A. Ivanova and D. I. Moldavanskii, "The residual π-finiteness of some one-relator groups", *Proc. Ivanovo State Univ. Mathematics*, vol. 6, 51–58, 2008.

[6] I. A. Pankratova, *Number-theoretic cryptography methods*. Tomsk State Univ., 2009.